IN THE CLAIMS:

Please amend claims 1, 27, and 37 as follows.

1. (Currently Amended) A method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network, the method including the steps of:

selectively routing, over ~~one of~~ said relatively insecure intermediate network ~~and~~ or said relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route said communication according to said information held in said storage means; and

encrypting said selectively routed communication by means of an encryption engine before it traverses said intermediate network,

wherein said at least one network element and said encryption engine are located substantially within said first secure network.

2. (Previously Presented) A method as in claim 1, wherein said at least one network element comprises switch means provided with control means and said storage means.

3. (Previously Presented) A method as in claim 2, wherein said storage means is operable to store said information comprising routing information.

4. (Previously Presented) A method as in claim 2 or 3, wherein said storage means is operable to store said information comprising security information.

5. (Previously Presented) A method as in claim 2, wherein said storage means is operable to store said information comprising security information including at least one of the following: encryption information; decryption information; security key information; and electronic cash information.

6. (Previously Presented) A method as in claim 3, wherein said switch means is operable to selectively route the predetermined type of communication according to routing information in said information held in the storage means.

7. (Previously Presented) A method as in claim 4, wherein said encryption engine is operable to encrypt said predetermined type of communication according to security information in said information held in said storage means.

8. (Previously Presented) A method as in claim 6, comprising the step of

identifying said predetermined type of communication by means of at least one of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics.

9. (Previously Presented) A method as in claim 8, wherein said predetermined type of communication is identified by means of originating and/or destination addresses.

10. (Previously Presented) A method as in claim 8, wherein said predetermined type of communication is identified by means of originating and/or destination identification numbers.

11. (Previously Presented) A method as in claim 4, wherein said storage means is operable to store said information comprising security information, said security information being distributed from a first node to at least one target node responsive to a predetermined trigger.

12. (Previously Presented) A method as in claim 3, wherein the stored routing information includes subscriber routing preferences.

13. (Previously Presented) A method as in claim 4, wherein the security information includes subscriber security preferences.

14. (Previously Presented) A method as in claim 4, wherein the security information includes encryption/decryption information defining a preferred algorithm or key for use with predetermined types of communication.

15. (Previously Presented) A method as in claim 2, wherein said information stored in the storage means is arranged to identify at least one group of users whose communications are to be routed and encrypted according to common preferences.

16. (Previously Presented) A method as in claim 2, further comprising providing a service management access point for accessing and changing said information held in the storage means.

17. (Previously Presented) A method as in claim 11, wherein said security information comprises decryption information, a distribution of said decryption information being triggered according to a predetermined schedule.

18. (Previously Presented) A method as in claim 11, wherein said security information is distributed to a node within at least one of the first and second secure networks.

19. (Previously Presented) A method as in claim 11, wherein said security information is distributed to an end terminal for the communication in question.

20. (Previously Presented) A method as in claim 11, wherein the at least one network element distributes said security information from a location substantially within the first secure network.

21. (Previously Presented) A method as in claim 11, wherein at least one network element distributes said security information from a location substantially within the second secure network.

22. (Previously Presented) A method as in claim 21, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route operated by trusted network operators.

23. (Previously Presented) A method as in claim 21, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route over said relatively insecure intermediate network.

24. (Previously Presented) A method according to claim 1, wherein said selectively routing step comprises providing said routing to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

25. (Canceled).

26. (Previously Presented) A method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, including the step of providing at least one network element operable to store security information and triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

27. (Currently Amended) A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network, the secure network arrangement including:

at least one network element triggerable to refer to information held in a storage means to selectively route over ~~one of~~ said relatively insecure intermediate network ~~and~~ or said relatively secure intermediate network a predetermined communication identified by a trigger according to said information held in said storage means from the first end terminal to the second end terminal over said relatively insecure intermediate network; and

an encryption engine for encrypting said selectively routed communication before it traverses said intermediate network,

wherein said at least one network element and said encryption engine are located substantially within said first secure network.

28. (Previously Presented) A secure network arrangement according to claim 27, wherein said at least one network element comprises a switch means provided with a control means and said storage means for storing said information including routing and encryption/decryption information.

29. (Previously Presented) A secure network arrangement according to claim 28, wherein the switch means is operable to selectively route said predetermined communication according to routing information held in the storage means and the encryption engine is operable to encrypt said selectively routed communication according to encryption information held in said storage means.

30. (Previously Presented) A secure network arrangement according to claim 29, wherein said predetermined communication is identified by means of at least one of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics and network service characteristics.

31. (Previously Presented) A secure network arrangement according to claim 30, wherein said predetermined communication is identified by means of an originating or destination address.

32. (Previously Presented) A secure network arrangement according to claim 31, wherein said predetermined communication is identified by means of originating identification or destination numbers.

33. (Original) A secure network arrangement according to claim 31, wherein the routing information and encryption/decryption information specifies operations according to subscriber preferences.

34. (Previously Presented) A secure network arrangement according to claim 33, wherein the encryption/decryption information defines a preferred algorithm or key for use with said predetermined communication.

35. (Previously Presented) A secure network arrangement according to claim 34, wherein the information held in the storage means identifies at least one group of users whose communications are to be routed and encrypted according to common preferences.

36. (Previously Presented) A secure network arrangement according to claim 27, comprising a service management access point for accessing and changing the information held in the storage means.

37. (Currently Amended) A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by at least intermediate network, wherein at least one communication route through which constitutes a relatively insecure communication route and at least one route constitutes a relatively secure communication route from the first end terminal to the second end terminal, the secure network arrangement including at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over ~~one of~~ said relatively insecure communication route ~~and~~ or said relatively secure communication route; and

an encryption engine for encrypting said selectively routed communication before it traverses said relatively insecure intermediate network, wherein said at least one

network element and said encryption engine are located substantially within said first secure network.

38. (Previously Presented) A secure network arrangement according to claim 37, including decryption means located substantially within the second secure network.

39. (Original) A secure network arrangement according to claim 38, wherein said decryption means are provided at the second end terminal.

40. (Original) A secure network arrangement according to claim 38, wherein said decryption means are provided at a node other than the second end terminal.

41. (Previously Presented) A method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, the method comprising providing at least one network element operable to store security information and being triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

42. (Previously Presented) A network arrangement for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, the network arrangement comprising at least one network element operable to store security information and triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

43. (Previously Presented) A network arrangement according to claim 42, wherein said network arrangement is operable to distribute said security information including at least one of encryption algorithms; decryption algorithms; security keys; and electronic cash bit strings.

44. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element comprises switch means provided with control means, and storage means for storing said encryption/decryption information.

45. (Previously Presented) A network arrangement according to claim 42, wherein said switch means is operable to selectively distribute said security information in response to a predetermined type of communication.

46. (Original) A network arrangement according to claim 45, wherein said predetermined type of communication is identified by means of originating subscriber characteristics, destination subscriber characteristics, payload characteristics or network service characteristics.

47. (Previously Presented) A network arrangement according to claim 42, wherein said distribution is triggered according to a predetermined schedule.

48. (Previously Presented) A network arrangement according to claim 42, comprising a service management access point.

49. (Previously Presented) A network arrangement according to claim 42, wherein the security information is distributed to a node within at least one of the first secure network and second secure network, rather than a destination end terminal for the communication in question.

50. (Previously Presented) A network arrangement according to claim 42, wherein the security information is distributed to an end terminal for the communication in question.

51. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element distributes said security information from a location substantially within the first secure network.

52. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element distributes the security information from a location substantially within at least one of the first or second networks.

53. (Previously Presented) A network arrangement according to claim 52, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route operated by trusted network operators.

54. (Previously Presented) A network arrangement according to claim 53, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route over the relatively insecure intermediate network.

55. (Canceled).

56. (Previously Presented) A network arrangement for the distribution of security

information between a node in a first secure network and at least one node in a second secure network, said first and second networks being separated by a relatively insecure intermediate network, including:

in at least one of said first and second secure networks, at least one network element operable to store security information and triggerable to distribute said security information to at least one or more target node in said second secure network; and

an encryption engine for encrypting a communication before it traverses said relatively insecure intermediate network.

57. (Canceled)

58. (Canceled)

59. (Previously Presented) A method according to claim 16, wherein said providing comprises providing said access point to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.